## CLAIMS

What is claimed is:

1. A system comprising:

a number generator to generate a nonce; and

an encryption subsystem to encrypt data accessed from a storage medium containing a key distribution data block using an encryption bus key prior to transmitting the encrypted data via a data bus, wherein said encryption bus key is derived based on at least a portion of the key distribution data block, at least one device key assigned to said encryption subsystem and the nonce generated by the number generator.

2. The system of claim 1, further comprising a decryption subsystem coupled to said data bus to decrypt said encrypted data received over the data bus using a decryption bus key derived based on at least a portion of the key distribution data block, at least one device key assigned to said decryption subsystem and the nonce generated by the number generator.

3. The system of claim 1, wherein said encryption subsystem comprises:

a processing logic to process at least a portion of the key distribution data block read from the storage medium using the at least one device key assigned to said encryption subsystem to compute a media key;

a one-way function to generate the encryption bus key based on the media key and the nonce generated by the number generator; and

an encryption logic to encrypt data accessed from said storage medium using said encryption bus key.

4. The system of claim 2, wherein said decryption subsystem comprises:

a processing logic to process at least a portion of the key distribution data block read from the storage medium using the at least one device key assigned to said decryption subsystem to compute a media key;

a one-way function to generate the decryption bus key based on said media key and the nonce generated by the number generator; and

a decryption logic to decrypt data transmitted over the data bus by using said decryption bus key.

5. The system of claim 1, wherein said data transmitted over the data bus is encrypted using the bus key derived based on the nonce generated by the number generator such that if said data is recorded at the time of transmission, said recorded data is not subsequently playable by a decryption subsystem that does not have access to the same nonce used by said encryption subsystem to encrypted said data transmitted over the data bus.

6. The system of claim 2, wherein said key distribution data block is embodied in the form of a media key block comprising a block of encrypted data.

7. The system of claim 2, wherein said encryption subsystem is implemented in a storage device capable of accessing data from a storage medium and said decryption subsystem is implemented in a host device capable of retrieving data from said storage device.

8. The system of claim 2, wherein said media key computed by the said encryption subsystem will be the same as the media key computed by the decryption subsystem provided that neither the device key assigned to the encryption subsystem nor the device key assigned to the decryption subsystem have been compromised.

9. The system of claim 2, wherein said storage medium is selected from a digital versatile disc (DVD), CD-ROM, optical disc, magneto-optical disc, flash-based memory, magnetic card and optical card.

10. The system of claim 2, wherein said number generator is a random number generator residing within said decryption subsystem.

11. A method comprising:

a storage device reading a key distribution data block from a storage medium;

the storage device processing at least a portion of said key distribution data block using at least one device key to compute a media key;

the storage device fetching a nonce generated by a number generator;

the storage device combining said nonce with said media key using a

one-way function to generate a bus key;

the storage device encrypting data read from the storage medium using the bus key generated by the storage device; and

the storage device transmitting the encrypted data over a data bus.

12. The method of claim 11, wherein said data transmitted over the data bus is encrypted using the bus key derived based on the nonce generated by the number generator such that if said data is recorded at the time of transmission, said recorded data is not subsequently playable by a host device that does not have access to the same nonce used by the storage device to encrypted said data transmitted over the data bus.

13. The method of claim 11, further comprising decrypting the encrypted data received over the data bus.

14. The method of claim 13, wherein said decrypting the encrypted data received over the data bus comprises:

a host device reading the key distribution data block from the storage medium;

the host device processing at least a portion of the key distribution data block using at least one device key to compute a media key;

the host device fetching the nonce generated by the number generator;

the host device combining said media key with the nonce using a one-way function to generate a bus key; and

the host device decrypting said encrypted data received over the data bus using the bus key generated by the host device.

15. The method of claim 14, further comprising:

the host device requesting a descramble key required for descrambling scrambled content from said storage device;

the storage device encrypting said descramble key read from said storage medium with said bus key generated by said storage device and sending said encrypted descramble key to the host device;

the host device decrypting said encrypted descramble key received from said storage device using said bus key generated by said host device.

the host device descrambling said decrypted data using said descramble

key decrypted by said host device.

16. The method of claim 11, wherein said key distribution data block is embodied in the form of a media key block comprising a block of encrypted data.

17. The method of claim 14, wherein said number generator is a random number generator residing within the host device.

18. An apparatus comprising:

a storage device to access a storage medium containing data and a key distribution data block, said storage device including a processing logic, a one-way function and an encryption logic, wherein said processing logic processes at least a portion of said key distribution data block using a device key assigned to said storage device to compute a media key, said one-way function combines said media key with a nonce generated by a number generator to produce a bus key and said encryption logic encrypts said data accessed from said storage medium using said bus key prior to transmitting the encrypted data via a data bus.

19. The apparatus of claim 18, further comprising a host device coupled to said storage device via said data bus, said host device including a processing logic, a one-way function and a decryption logic, wherein said processing logic processes at least a portion of said key distribution data block using a device key assigned to said host device to compute a media key, said one-way function combines said media key with said nonce generated by said number generator to produce a bus key and said decryption logic decrypts said encrypted data received over the data bus using said bus key.

20. The apparatus of claim 18, wherein said data transmitted over the data bus is encrypted using the bus key derived based on the nonce generated by the number generator such that if said data is recorded at the time of transmission, said recorded data is not subsequently playable by a host device that does not have access to the same nonce used by said storage device to encrypted said data transmitted over the data bus.

21. The apparatus of claim 19, wherein said media key computed by the said storage device will be the same as the media key computed by the host device provided that neither the device key assigned to the storage device nor the device key assigned to the host device have been compromised.

22. The apparatus of claim 19, wherein said number generator is a random number generator residing within said host device.

23. The apparatus of claim 19, wherein said storage device is embodied in the form of a DVD drive and said host device is embodied in the form of either a DVD player or a personal computer.

24. The apparatus of claim 19, wherein said storage medium is selected from a digital versatile disc (DVD), CD-ROM, optical disc, magneto-optical disc, flash-based memory, magnetic card and optical card.

25. The apparatus of claim 19, wherein said storage medium is embodied in the form of a DVD containing scrambled content.

26. The apparatus of claim 19, wherein said key distribution data block is embodied in the form of a media key block comprising a block of encrypted data.